JOURNAL OF COMBINATORIAL THEORY (A) 22, 110–114 (1977)

Note

Pelikán's Conjecture and Cyclotomic Cosets

F. J. MACWILLIAMS AND A. M. ODLYZKO

Bell Laboratories, Murray Hill, New Jersey 07974

Communicated by the Managing Editors

Received January 21, 1976

The following conjecture was recently made by J. Pelikán.

Let $a_0,\ldots, a_n$ be an $(n+1)$-tuple of 0's and 1's; let $A_k = \sum_{i=0}^{n-k} a_i a_{i+k}$ for $k = 0,\ldots, n$. Then if $n \geqslant 4$ some A_k is even.

This paper shows that Pelikán's conjecture is false for infinitely many values of n. On the other hand it is also shown that the conjecture is true for most values of n, and a characterization is given of those values of n for which it fails.

1. INTRODUCTION

J. Pelikán [3] recently made a conjecture, which we rephrase as follows: Let $a_0,\ldots, a_n \in GF(2)$; let

$$A_k = \sum_{i=0}^{n-k} a_i a_{i+k}$$

(the sum to be evaluated in $GF(2)$) for $k = 0, 1,\ldots, n$. Then if $n \geqslant 4$ some A_k is zero.

In this paper we show that this conjecture is false, in fact we obtain the following results.

THEOREM. *A counterexample of length n to Pelikán's conjecture exists if and only if $2n+1 \in P$ where P is a nonempty set of odd positive integers, with the following properties.* (i) *An integer r belongs to P if and only if all the prime factors of r belong to P.* (ii) *If p is a prime, then $p \in P$ if and only if p divides $2^{2s+1} - 1$ for some s; in other words if and only if $\exp_p(2)$ is odd, where $\exp_p(a)$ is the smallest positive integer m such that $a^m \equiv 1 \bmod(p)$. This implies that if $p \equiv -1 \bmod(8)$ then $p \in P$, and if $p \equiv \pm 3 \bmod(8)$, then $p \notin P$.*

The last part of the theorem leaves open the question of the behavior of primes $p \equiv 1 \bmod(8)$. It turns out that these are sometimes in P and sometimes not; among primes $p \equiv 1 \bmod(8)$, $p < 1000$ only 73, 89, 233, 337, 601, 881, and 937 belong to P. For further results, see [1, 2]. In particular, it is shown there that the Dirichlet density of the primes $p \in P$, $p \equiv 1 \bmod(8)$, is 1/24. Using stronger versions of the Chebotarev density theorem it can even be shown that if $\pi_P(x) = |\{p \in P;\ p \text{ prime}, p \leqslant x\}|$, then

$$\pi_P(x) \sim (7/6)\,\pi(x; 8, 1) \sim (7/24)\,\pi(x) \qquad \text{as} \quad x \to \infty.$$

Since for every $r \in P$ all the prime factors p of r have to satisfy $p \equiv \pm 1 \bmod(8)$, we conclude that the asymptotic density of P is zero. Thus Pelikán's conjecture is almost always true.

It will be clear from the proof of the theorem that for those n for which $2n + 1 \in P$, all the counterexamples can be constructed quite easily, and that their number is a power of 2.

2. PRELIMINARIES

Recall that $a_0, a_1, \ldots, a_n \in GF(2)$, and

$$A_k = \sum_{i=0}^{n-k} a_i a_{i+k}\,.$$

Set

$$f(x) = \sum_{i=0}^{n} a_i x^i \in GF(2)[x].$$

Then

$$\begin{aligned} f(x)\,f(x^{-1}) &= \left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{j=0}^{n} a_j x^{-j}\right) \\ &= \sum_{i,j} a_i a_j x^{i-j} \\ &= \sum_{k=-n}^{n} x^k \sum_{i-j=k} a_i a_j \\ &= A_0 + \sum_{k=1}^{n} A_k (x^k + x^{-k}). \end{aligned}$$

Now suppose $A_i = 1$ for $0 \leqslant i \leqslant n$. Then

$$\begin{aligned} f(x)f(x^{-1}) &= 1 + \sum_{k=1}^{n} (x^k + x^{-k}) \\ &= x^{-n}(1 + x + \cdots + x^{2n}) \\ &= x^{-n}((x^{2n+1} + 1)/(x + 1)). \end{aligned}$$

Set $\hat{f}(x) = x^n f(x^{-1})$, then

$$f(x)\hat{f}(x) = ((x^{2n+1} + 1)/(x + 1)). \tag{1}$$

The right side is a polynomial of degree $2n$, and its $2n$ zeros are precisely the $(2n + 1)$st roots of unity, excluding 1.

Now if α is a zero of $f(x)$, then α^{-1} is a zero of $\hat{f}(x)$, and conversely. Since $f(x)$ and $\hat{f}(x)$ are polynomials over $GF(2)$, this condition makes it possible to determine all solutions to (1).

3. Factorization of $x^{2n+1} + 1$ over $GF(2)$

We first recall some standard terminology.

Let ξ be a primitive $(2n + 1)$st root of unity. Suppose $g(x)$ is an irreducible factor of $x^{2n+1} + 1$ over $GF(2)$. If α is a zero of $g(x)$, then $\alpha = \xi^a$ for some positive integer a. The other zeros of $g(x)$ are then precisely $\xi^{2a}, \xi^{4a}, \ldots, \xi^{a2^{k-1}}$ where k is the smallest positive integer such that $2^k a \equiv a \bmod(2n + 1)$.

This result motivates the definition of cyclotomic cosets. The cyclotomic coset of $a \bmod(2n + 1)$, which we call C_a, consists of the numbers

$$a, 2a, 4a, \ldots, a2^{k-1}$$

(all reduced $\bmod(2n + 1)$). Of course $C_a = C_{2a} = C_{4a} = \cdots$. The irreducible factors of $x^{2n+1} + 1$ over $GF(2)$ are the polynomials

$$g_a(x) = \prod_{i \in C_a} (x + \xi^i).$$

Now factor $f(x)$ into irreducible factors

$$f(x) = \prod_{a \in A} g_a(x)$$

where the cyclotomic cosets for $a \in A$ are distinct. Then it must be that

$$\hat{f}(x) = \prod_{a \in A} g_{-a}(x).$$

Since (1) holds, any nontrivial $(2n+1)$st root of unity is a zero of exactly one of $f(x), \hat{f}(x)$. This implies that (1) can happen if and only if a and $-a$ are never in the same cyclotomic coset mod$(2n+1)$, for $1 \leqslant a \leqslant 2n$.

EXAMPLE. For $n = 11$, the cyclotomic costes mod 23 are

$$C_0 = \{0\},$$
$$C_1 = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\},$$
$$C_5 = \{5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22\}.$$

Thus in this case there is a solution to (1) and a counterexample to Pelikán's conjecture. This is given by the coefficients of the polynomial

$$f(x) = \prod_{i \in C_1} (x - \xi^i), \qquad \text{i.e., } a_0, \ldots, a_{11} = 101011100011.$$

Thus the question of when Pelikán's conjecture fails is reduced to the question of finding the numbers n such that a and $-a$ are in distinct cyclotomic cosets mod$(2n+1)$ for all a, $1 \leqslant a \leqslant 2n$. Moreover for such n, if the number of cyclotomic cosets mod$(2n+1)$ is $2h+1$ (including the trivial coset $\{0\}$), then there will be 2^h counterexamples to the conjecture.

4. STRUCTURE OF THE CYCLOTOMIC COSETS

Let P denote the set of odd integers $r \geqslant 3$ for which the cyclotomic cosets mod r satisfy the condition that a and $-a$ mod(r) are never in the same cyclotomic coset for $1 \leqslant a \leqslant r-1$. We study the conditions under which $r \in P$.

Consider first the case where $r = p$, a prime. Then $C_a = aC_1 = \{a2^i \pmod p, 2^i \in C_1\}$; thus $-a \in C_a$ if and only if $-1 \in C_1$, i.e., if and only if $2^k \equiv -1 \bmod(p)$ for some k. Now suppose $m = \exp_p(2)$ (the smallest positive integer such that $2^m \equiv 1 \bmod(p)$). If m is even, say $m = 2m'$, then

$$2^{2m'} - 1 = (2^{m'} - 1)(2^{m'} + 1) \equiv 0 \mod(p),$$

and so $2^{m'} + 1 \equiv 0 \bmod(p)$ by minimality of m. Thus $p \notin P$ in this case. On the other hand, if $2^k \equiv -1 \bmod(p)$, then $2^{2k} \equiv 1 \bmod(p)$ and so m divides $2k$. If m is odd this implies m divides k, which is patently false. Thus the primes $p \in P$ are precisely those for which $\exp_p(2)$ is odd. They are the primes which divide $2^{2s+1} - 1$ for some s.

If $p \equiv -1 \bmod(8)$ then 2 is a quadratic residue, and since the number of quadratic residues is odd, $\exp_p(2)$ is odd. If $p \equiv \pm 3 \bmod(8)$ then 2 is a nonresidue, i.e., if g is a primitive root of p, $2 \equiv g^{2s+1}$, and $\exp_p(2) = (p-1)/\gcd(p-1, 2s+1)$, which is even. This leaves open the case $p \equiv 1 \bmod(8)$, in which case $\exp_p(2)$ can be odd or even, although the odd case is rare.

Now consider the general case. Suppose $p \in P$. If $p^i \notin P$ for some $i > 1$, then $2^k a \equiv -a \bmod(p^i)$, i.e., $(2^k+1)a \equiv 0 \bmod(p^i)$ for some a, $1 \leqslant a < p^i - 1$. But $p \in P$, so p does not divide $2^k + 1$, i.e., p^i divides a, which is impossible.

Now suppose $r, s \in P$ and r and s are relatively prime. If $rs \notin P$, then $2^k a \equiv -a \bmod(rs)$ for some a, $1 \leqslant a \leqslant rs - 1$. Then $rs \mid (2^k+1)a$. Since r, $s \in P$ we must have $r \mid a$, $s \mid a$, thus $rs \mid a$, a contradiction. Hence $rs \in P$. Thus if $r = \prod p_i^{a_i}$, where $p_i \in P$ for all i, then $p_i^{a_i} \in P$ for all i, and since the $p_i^{a_i}$ are relatively prime, we conclude $r \in P$.

Finally suppose $r \notin P$ and s is any positive integer. Since $r \notin P$ there is an a such that $2^k a \equiv -a \bmod(r)$ $1 \leqslant a \leqslant r - 1$. Then $2^k as \equiv -as \bmod(rs)$, $1 \leqslant as \leqslant rs - 1$. Thus $rs \notin P$.

The preceding paragraph shows that if $r \in P$ and d divides r, then $d \in P$. Thus if $r \in P$, all the prime divisors of r are in P, which completes the proof.

REFERENCES

1. P. FEIN, B. GORDON, AND J. H. SMITH, On the representation of -1 as a sum of two squares in an algebraic number field, *J. Number Theory* **3** (1971), 310–315.
2. H. HASSE, Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von durch eine vorgegebene Primzahl $\ell \neq 2$ teilbarer bzw. unteilbarer Ordnung mod. p ist, *Math. Ann.* **162** (1965), 74–76.
3. A. HAJNAL, R. RADO, V. T. SÓS, (Eds.), "Infinite and Finite Sets (Proceedings of the 10th Bolyai Colloquium, Dedicated to P. Erdös)," Vol. III, p. 1549, North-Holland, Amsterdam, 1975.